Symantec™ ServiceDesk 7.5 Release Notes

Symantec™ ServiceDesk 7.5 Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec™ ServiceDesk 7.5 Release Notes

This document includes the following topics:

ServiceDesk 7.5.1 update notes

ServiceDesk 7.5.1 is an update to ServiceDesk 7.5. This update corrects several issues in the Change Management process. This update also corrects an issue with the ServiceDesk MSI installer.

Symantec recommends updating to ServiceDesk 7.5.1.

If you have already installed ServiceDesk 7.5.0, Symantec recommends using a separately provided Change Management process installer to apply the update. For more information, refer to the knowledge base article *ServiceDesk 7.5.1 update* at http://www.symantec.com/docs/HOWTO83330.

If you plan to install ServiceDesk 7.5 for the first time, for installation or migration information, refer to the Symantec™ ServiceDesk 7.5 Implementation Guide at http://www.symantec.com/docs/DOC5722.

See "Installing ServiceDesk 7.5" on page 18.

See "Migrating to ServiceDesk 7.5" on page 19.

For more information about the fixed issues in this update, see the *Fixed Issues* section.

See "Fixed issues " on page 28.

About ServiceDesk 7.5

Symantec ServiceDesk improves your infrastructure's service management.

It is ITIL-based and includes all of the primary ITIL Service Management processes. These processes include Incident Management, Problem Management, Change Management, and Knowledge Management. ServiceDesk also includes a Service Catalog that lets your users choose service items. It also includes an Active Directory Self Service Catalog that lets users easily and securely reset passwords and access network shares.

ServiceDesk uses the Symantec Workflow framework to manage service tickets, provide reports, and integrate with the Configuration Management Database (CMDB).

You can configure ServiceDesk to meet your organization's specific requirements. These configurations include setting up business hours, routing rules for incidents and changes, and email templates and notification rules. You can implement advanced customizations. These customizations may include creating data types, modifying feeder forms, modifying the Process View page, and adding fields to reports.

For more information, see the following:

Symantec™ ServiceDesk 7.5 Implementation Guide

Symantec™ ServiceDesk 7.5 User Guide

For videos and articles, join the Symantec sponsored ServiceDesk user group on Symantec Connect:

http://www.symantec.com/connect/groups/symantec-servicedesk

For continuous documentation updates, subscribe to the following forum on Symantec Connect:

www.symantec.com/connect/endpoint-management/

See "What's new in ServiceDesk 7.5" on page 6.

See "Installing ServiceDesk 7.5" on page 18.

See "Migrating to ServiceDesk 7.5" on page 19.

What's new in ServiceDesk 7.5

In the 7.5 release of ServiceDesk, the following new features are introduced:

Table 1-1   List of new features in ServiceDesk 7.5

Feature	Description
Support for Microsoft SQL Server 2008 and 2012	SQL Server 2008 SP3, SQL Server 2008 R2 SP2, and SQL Server 2012 are now supported.
Symantec Management Platform (for ServiceDesk)	ServiceDesk supports the Symantec Management Platform version 7.1 SP2 and version 7.5.
New installation utility	The new ServiceDesk installer simplifies the ServiceDesk install.
	A new wizard guides you through the following steps:
	■ Download of the Workflow installation file ■ Installation of the Workflow Platform ■ Installation of the ServiceDesk modules

Table 1-1   List of new features in ServiceDesk 7.5 *(continued)*

Feature	Description
Ability to select which ServiceDesk Modules (processes) to install	The new installer lets you install any or all of the following ServiceDesk processes: ■ **Change Management** ■ **Incident Management** ■ **Problem Management** ■ **Knowledge Base Management** ■ **Active Directory Self Service Catalog**
Improved ServiceDesk Implementation Guide	The *Symantec™ ServiceDesk 7.5 Implementation Guide* includes the following information: ■ Planning and preparing for the installation ■ ServiceDesk scalability and performance tuning ■ ServiceDesk installation ■ Advance customizations For more information, see Symantec™ ServiceDesk 7.5 Implementation Guide.
The Administrator can configure business hours within the Process Manager portal.	Business hours can be configured from the **Business Hours** page in the Process Manager portal. To access the **Business Hours** page, click **Admin > Data > Business Hours**.
The Administrator can configure Service Level Agreements (SLAs) within the Process Manager portal.	SLA Levels, SLA Escalations, and SLA Milestones can be managed from the **Automation Rules** page in the Process Manager portal. To access the **Automation Rules** page, click **Admin > Process Automation**, then expand **Incident Management**, and click **Service Dashboard**.
Improved Service Level Agreement time span selection.	Service Level Agreements can be configured for longer time spans.

Table 1-1   List of new features in ServiceDesk 7.5 *(continued)*

Feature	Description
The Administrator can manage data mapping within the Process Manager portal,.	Data mapping classifications can be used to set up your Routing Table from the **Data Mapping** page in the Process Manager portal. To access the **Data Mapping** page, click **Admin > Process Automation**. Then expand **Incident Management**, click **Service Dashboard**, and then click **Manage Data Mapping**.
New Incident Management process	Features of the new Incident Management process are as follows: ■ Expanded the number of out-of-the-box rulesets. ■ Incidents are routed to Service Queues instead of users or groups. ■ Ability to create email templates for data and process events ■ Ability to create routing rules to route emails for data and process events ■ Ability to evoke Workflow from an Incident Management ruleset
Additions to Change Management process	Additions to the Change Management process are as follows: ■ Ability to route change request by risk score ■ Ability to create email templates for data and process events ■ Ability to create routing rules to route emails for data and process events ■ Ability to evoke Workflow from a Change Management ruleset
Improved the reopening a closed incident process.	Improvements to the reopening a closed incident process are as follows: ■ A new ticket is created for the reopened incident. ■ A reference is provided to the original incident. ■ Ability to assign the ticket to a specific worker or service queue

Table 1-1   List of new features in ServiceDesk 7.5 *(continued)*

Feature	Description
New Web Part for the Technicians for viewing SLA Status	Technicians can view the SLA Status for initial response and resolution in a separate Web Part from within the Incident ticket's **Process View** page. The Web Part is located in the upper right of the **Process View** page.
New Web Part for the Technicians for viewing the user comments separate from the Process History	Technicians can view the user comments in a separate Web Part from within the Incident ticket's **Process View** page. The Web Part is located on the left side of the page.
Technicians have the ability to change incident details.	Technician cans change incident details, which include the extended classifications, when they work in incident.

See "Installing ServiceDesk 7.5" on page 18.

See "Migrating to ServiceDesk 7.5" on page 19.

ServiceDesk 7.5 support matrix

The support matrix provides an overview of the primary ServiceDesk components and their supported operating systems. It displays the versions of the operating systems that are supported and the versions that are not supported in ServiceDesk 7.5.

See "System requirements for ServiceDesk" on page 11.

Table 1-2   ServiceDesk support matrix

Component	Supported in ServiceDesk 7.5	Support new to ServiceDesk 7.5	Not Supported in ServiceDesk 7.5
Symantec Management Platform (for ServiceDesk)	■ 7.1 SP2 ■ 7.5	■ 7.5	■ 7.1 ■ 7.1 SP1
ServiceDesk Server/Process Manager portal operating system (OS)	■ Windows Server 2008 R2 SP1 x64 Symantec recommends that you use this OS.	N/A	■ Windows Server 2003 (all versions) ■ Windows Server 2008 (pre-R2) ■ Windows Server 2008 R2

Table 1-2   ServiceDesk support matrix *(continued)*

Component	Supported in ServiceDesk 7.5	Support new to ServiceDesk 7.5	Not Supported in ServiceDesk 7.5
Microsoft SQL Server	▪ Microsoft SQL Server 2005 SP4 ▪ Microsoft SQL Server 2008 SP2 ▪ Microsoft SQL Server 2008 SP3 ▪ Microsoft SQL Server 2008 R2 SP1 ▪ Microsoft SQL Server 2008 R2 SP2 ▪ Microsoft SQL Server 2012	▪ Microsoft SQL Server 2008 SP3 ▪ Microsoft SQL Server 2008 R2 SP2 ▪ Microsoft SQL Server 2012	▪ Microsoft SQL Server 2005 SP2 ▪ Microsoft SQL Server 2005 SP3 ▪ Microsoft SQL Server 2008 ▪ Microsoft SQL Server 2008 SP1
Workflow Designer operating system (OS)	▪ Windows XP SP3 x86 ▪ Windows 7 x86 and x64 ▪ Windows 7 SP1 x86 and x64 ▪ All Workflow Server supported OS versions	N/A	▪ Windows XP SP2 ▪ Windows Vista SP1 ▪ Windows Vista SP2 x86 and x64
Process Manager portal browsers	▪ Microsoft Internet Explorer versions 7, 8, and 9 **Note:** Active Directory auto-authentication is only supported with Internet Explorer. ▪ Firefox version 13 and later ▪ Google Chrome version 17 and later ▪ Safari version 5 and later	N/A	N/A

System requirements for ServiceDesk

ServiceDesk requires that you dedicate certain servers.

You can use any of several configurations for setting up the Symantec Management Platform, the ServiceDesk server, and the SQL Server.

See "Server configuration options for ServiceDesk" on page 16.

<p align="center">**Table 1-3**   The dedicated servers that ServiceDesk requires</p>

Server	Description
Symantec Management Platform	ServiceDesk requires a 7.1 SP2 instance or a 7.5 instance of the Symantec Management Platform. See "ServiceDesk requirements for the Symantec Management Platform" on page 11.
ServiceDesk server	The ServiceDesk server is a 64-bit server on which you install the Workflow Platform and the ServiceDesk modules. This server might also be referred to as the Process Manager server or the Workflow Server. This server cannot contain an installation of Helpdesk Solution. See "System requirements for the ServiceDesk server" on page 12.
SQL Server	The Process Manager databases must reside on a SQL Server. Symantec recommends that ServiceDesk has its own dedicated off-box SQL Server. See "System requirements for the SQL Server" on page 14. See "About supported SQL Server collations for the Process Manager database" on page 15.

See "Requirements for the ServiceDesk client computers" on page 16.

ServiceDesk requirements for the Symantec Management Platform

ServiceDesk requires a 7.1 SP2 instance or a 7.5 instance of the Symantec Management Platform to be installed and running. The Symantec Management Platform must always be installed on its own 64-bit server.

| Table 1-4 | ServiceDesk requirements for the Symantec Management Platform |

Item	Requirement
Hardware and base software	▪ For information about the Symantec Management Platform 7.1 SP2 hardware and the software requirements, see the chapter *Performance and scalability recommendations for IT Management Suite* in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide. ▪ For information about the Symantec Management Platform 7.5 hardware and the software requirements, see the chapter *Hardware recommendations* in the Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Installation and Upgrade Guide.
Symantec Management Platform	A 7.1 SP2 instance or a 7.5 instance of the Symantec Management Platform must be installed and running. The installation of your instance of the Symantec Management Platform is managed through the Symantec Installation Manager.
Altiris Configuration Management Database Solution (CMDB Solution)	If the Configuration Management Database Solution is not already installed, it is included in the installation of the ServiceDesk solution software. You do not need to perform a separate installation.

System requirements for the ServiceDesk server

The ServiceDesk software is installed on the ServiceDesk server. This server cannot contain an installation of Helpdesk Solution.

When you install the ServiceDesk software and SQL Server on different servers, the servers must meet the following requirements:

▪ Both servers must be members of the same domain.

▪ This configuration must be installed in an Active Directory environment.

| Table 1-5 | System requirements for the ServiceDesk server |

Item	Requirement
Server and processor	Multi-core or multiple processors, 64-bit
RAM	▪ Minimum: 8 GB (recommended for test servers only) ▪ Minimum recommended: 16 GB ▪ Preferred: 32 GB
Operating system	Windows Server 2008 R2 SP1, 64 bit

Table 1-5   System requirements for the ServiceDesk server *(continued)*

Item	Requirement
Network configuration	- IP v4 - Static IP address - Name resolution services (DNS) - Internet connectivity - Connectivity to the Symantec Management Platform server - Gigabit Network Interface Controller (GB NIC)
Installation account	ServiceDesk requires an installation account: ■ **Windows** (Windows Integrated Security) Use a domain account with the *sysadmin* server role on the target SQL instance. ■ **SQL** (Microsoft SQL Server Security) Use a SQL account with the *sysadmin* server role for that target SQL instance. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Operation service account	ServiceDesk requires a run-time service account. ■ **Windows** (Windows Integrated Security) Use a domain service account that is set up in that SQL instance. This account is used as the identity under which the ServiceDesk application pool runs in IIS. This account is added to the *db_owner* role on the Process Manager database. **Note:** This authentication method is the recommended authentication method. Windows authentication allows for easy upgradeability and provides the greatest ease of change. Because connection string information is stored in the Web.config files of Projects, Windows authentication also adds security. ■ **SQL** (Microsoft SQL Server Security) Use an account in the target SQL instance. This account is added to the *db_owner* role on the Process Manager database. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Email account	- Primary email account for the ServiceDesk mailbox for monitoring the system and sending email from the system - SMTP server connectivity (Optional) POP or IMAP mailbox for monitoring

Table 1-5   System requirements for the ServiceDesk server *(continued)*

Item	Requirement
SQL Server components	The ServiceDesk server requires the SQL Server ADOMD.NET. This SQL Server component is a Microsoft .NET Framework data provider. It facilitates communication with the Microsoft SQL Server Analysis Services.
	If SQL Server is installed on a server that is separate from the ServiceDesk server (off-box), the ServiceDesk server requires the following SQL Server components:
	■ SQL Management Objects (SMO) site ■ SQL Server Analysis Management Objects (AMO) ■ Microsoft ADOMD.NET ■ SQL Native client This component is a prerequisite for installing the SQL Management Objects.
Microsoft Internet Information Services (IIS)	IIS 7 (IIS 6 Management Compatibility mode)
.NET Framework	.NET 3.5 with ASP.NET
Internet browser	ServiceDesk is intended to work with all of the major Internet browsers.
	We have tested ServiceDesk with the following browsers:
	■ Microsoft Internet Explorer versions 7, 8, and 9 **Note:** Active Directory auto-authentication is only supported with Internet Explorer. ■ Firefox version 13 and later ■ Google Chrome version 17 and later ■ Safari version 5 and later

You can use any of several configurations for setting up the Symantec Management Platform, the ServiceDesk server, and the SQL Server.

System requirements for the SQL Server

ServiceDesk requires an installation of Microsoft SQL Server.

When you install the ServiceDesk software and SQL Server on different servers, the servers must meet the following requirements:

■ Both servers must be members of the same domain.

■ This configuration must be installed in an Active Directory environment.

Table 1-6 System requirements for the SQL Server

Item	Requirement
Processor	32-bit or 64-bit Symantec recommends that you use a 64-bit.
Operating system	Windows Server 2008 R2 SP1
Database	Microsoft SQL Server Supported versions of SQL Server: ■ SQL Server 2005 SP4 ■ SQL Server 2008 SP2 or 2008 SP3 ■ SQL Server 2008 R2, 2008 R2 SP1, or 2008 R2 SP2 ■ SQL Server 2012
Database	ServiceDesk requires the following components of Microsoft SQL Server: ■ SQL Server Reporting Services ■ SQL Server Analysis Services
Additional requirements	When you use one SQL Server for both the Symantec Management Platform and the ServiceDesk software, follow the Symantec Management Platform's SQL Server requirements. ■ For information about the Symantec Management Platform 7.1 P2 recommended hardware configurations, see the chapter *Performance and scalability recommendations for IT Management Suite* in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide. ■ For information about the Symantec Management Platform 7.5 recommended hardware configurations, see the chapter *Hardware recommendations* in the Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Installation and Upgrade Guide.

You can use any of several configurations for setting up the Symantec Management Platform, the ServiceDesk server, and the SQL Server.

See "Server configuration options for ServiceDesk" on page 16.

See "System requirements for ServiceDesk" on page 11.

About supported SQL Server collations for the Process Manager database

The Process Manager database supports the following SQL Server collations:

■ SQL_Latin1_General_CP1_CI_AS - Latin alphabet, case insensitive, accent sensitive
By default, the Process Manager database is created with this collation.

- SQL_Latin1_General_CP1_CS_AS - Latin alphabet, case sensitive, accent sensitive

  If during installation the user checks the option to make the database case sensitive, the Process Manager database is created with this collation.

See "System requirements for ServiceDesk" on page 11.

Requirements for the ServiceDesk client computers

The client computers access ServiceDesk from an Internet browser. ServiceDesk is intended to work with all the major Internet browsers.

We have tested ServiceDesk with the following browsers:

- Microsoft Internet Explorer versions 7, 8, and 9

Note: Active Directory auto-authentication is only supported with Internet Explorer.

- Firefox version 13 and later
- Google Chrome version 17 and later
- Safari version 5 and later

See "System requirements for ServiceDesk" on page 11.

Server configuration options for ServiceDesk

The ServiceDesk installation requires that you dedicate certain servers: a Symantec Management Platform, a ServiceDesk server, and a SQL Server.

See "System requirements for ServiceDesk" on page 11.

The server configuration that you use for a ServiceDesk installation depends on your environment, datacenter design, and budget.

Requirements for server configurations

A server configuration is valid if it meets the following requirements:

- Microsoft SQL Server is installed on either a 32-bit server or a 64-bit server.

  Symantec recommends that you use a 64-bit server.
- The Symantec Management Platform and the ServiceDesk Solution software are installed on a 64-bit server.
- ServiceDesk is installed on a 64-bit server.

  Separate from the Symantec Management Platform

Typical server configurations	The most commonly-used configurations are as follows:

■ SQL Server is installed off-box for both the Symantec Management Platform and ServiceDesk.
See Figure 1-1.

■ The Symantec Management Platform and ServiceDesk share an off-box SQL Server installation.
See Figure 1-2.

Additional server configurations	Examples of additional configurations are as follows:

■ SQL Server is installed off-box for either the Symantec Management Platform or ServiceDesk.

■ SQL Server is installed on-box for either the Symantec Management Platform or ServiceDesk, or both.

■ One of the applications uses an on-box installation of SQL Server and shares it with the other application.

■ One of the applications uses an on-box installation of SQL Server and the other application uses an off-box installation of SQL Server.

Unsupported server configurations	Symantec does not support the following server configuration:

■ Symantec Management Platform with ServiceDesk Solution software installed on the same server as the ServiceDesk application software.

Note: The Symantec Management Platform with ServiceDesk Solution must be installed to a separate server than the actual ServiceDesk application server.

Figure 1-1   Both Symantec Management Platform and ServiceDesk have their own off-box SQL Server
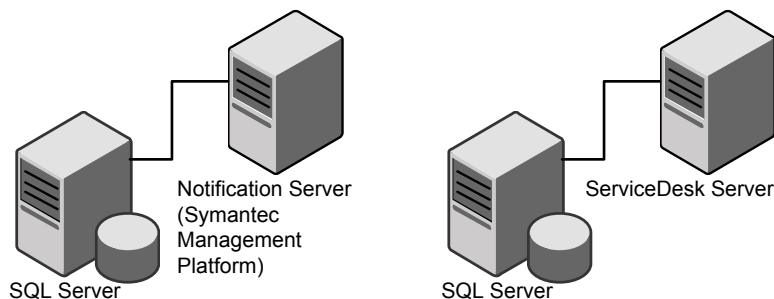
Figure 1-2   Symantec Management Platform and ServiceDesk share an off-box
SQL Server

Notification Server
(Symantec
Management
Platform)

SQL Server

ServiceDesk Server
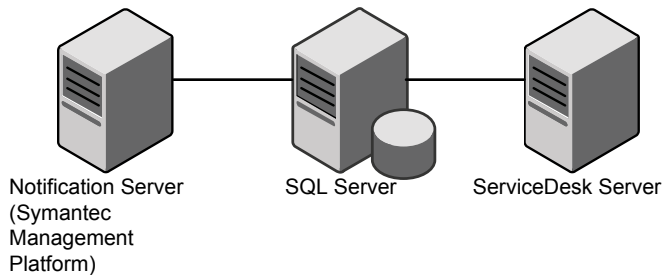
Installing ServiceDesk 7.5

You can install ServiceDesk as a standalone product. You can also install
ServiceDesk and use it along with the other products in the IT Management Suite.

Before you install ServiceDesk on the ServiceDesk server, read the section
"ServiceDesk scalability" in the *Symantec™ ServiceDesk 7.5 Implementation Guide*
at the following URL:

http://www.symantec.com/docs/DOC5722

Things to know about the ServiceDesk installation process:

■ You use the Symantec Installation Manager (SIM) to install the ServiceDesk
   solution software.
   ServiceDesk is compatible with Symantec Management Platform 7.1 SP2, 7.1
   SP2 MP1, and 7.5. ServiceDesk is also compatible with IT Management Suite
   7.1 SP2, 7.1 SP2 MP1, and 7.5.

■ You use the ServiceDesk server installer to install the ServiceDesk application
   on your new designated server.
   SIM does not install ServiceDesk on the ServiceDesk server. SIM installs the
   ServiceDesk solution software. The ServiceDesk solution software grants you
   access to the ServiceDesk Server installer.

For information about installing ServiceDesk, see the *Symantec™ ServiceDesk 7.5
Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC5722.

For information about installing IT Management Suite 7.1 SP2, see the *Altiris™ IT
Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide*
at the following URL:

http://www.symantec.com/docs/DOC4827

For information about installing IT Management Suite 7.5, see the *Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC5670

See "About ServiceDesk 7.5" on page 5.

See "Migrating to ServiceDesk 7.5" on page 19.

Migrating to ServiceDesk 7.5

Existing ServiceDesk customers must migrate to ServiceDesk 7.5, which involves migrating to new hardware. This migration includes both the ServiceDesk server and a new database instance. You should plan to install ServiceDesk in a new environment, separate from your existing ServiceDesk server. An in-place upgrade path is not available, and Symantec does not support attempts to install 7.5 over a previous version of ServiceDesk. You are required to run both systems in parallel until your previous tickets are closed and necessary data is migrated to your ServiceDesk 7.5 environment.

Things to know about the ServiceDesk migration process:

■ Symantec Management Platform (and IT Management Suite if installed) must first be upgraded or migrated to version 7.1 SP2 or version 7.5.
ServiceDesk 7.5 is compatible with Symantec Management Platform 7.1 SP2, 7.1 SP2 MP1, and 7.5.

■ You use the ServiceDesk Server installer to install the ServiceDesk application on your new designated server.
Symantec Installation Manager (SIM) does not install ServiceDesk on the ServiceDesk server. SIM installs the ServiceDesk solution software. The ServiceDesk solution software grants you access to the ServiceDesk Server installer.

For information about migrating to ServiceDesk 7.5, see the section "Migrating to ServiceDesk 7.5" in the *Symantec™ ServiceDesk 7.5 Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4798

For more information about upgrading or migrating to Symantec Management Platform 7.1 SP2, see the section *About upgrading from IT Management Suite 7.1 to 7.1 SP2* in the *Symantec™ Management Platform 7.1 SP2 Installation Guide* at the following URL:

http://www.symantec.com/docs/DOC4798

For more information about upgrading or migrating to Symantec Management Platform 7.5, see the chapter *Upgrading to IT Management Suite 7.5* or *Migrating to IT Manatement Suite 7.5* in the *Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC5697

Migrating data to ServiceDesk 7.5

You can leverage some of the data from ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 in ServiceDesk 7.5. You can migrate incidents, change requests, problems, and other data. You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.

You can also leverage some data from Helpdesk Solution 6.x. You can migrate incidents, categories, and some knowledge base content.

For more information about migrating data to ServiceDesk 7.5, see the section "About migrating data to ServiceDesk 7.5" in the *Symantec™ ServiceDesk 7.5 Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC5722

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

Table 1-7   Known issues

Issue	Description	Article link
A new ServiceDesk installation fails if you do not close the ServiceDesk installation wizard after you run an uninstall.	Using the ServiceDesk installer to uninstall ServiceDesk and/or Workflow and then to reinstall ServiceDesk without closing the installer after the uninstall causes error during reinstallation. **Workaround:** After using the ServiceDesk installer to uninstall ServiceDesk and/or Workflow, close the ServiceDesk installer before using it to reinstall ServiceDesk.	
You cannot use *SQL 2008 R2 Datacenter* edition to build your SQL Server.	If you attempt to install ServiceDesk 7.5 to *SQL Server 2008 R2 Datacenter* edition, the prerequisite check fails and you cannot continue. **Workaround:** Do not use *SQL 2008 R2 Datacenter* edition to build your SQL Server. *SQL 2008 R2 Datacenter* is currently unsupported.	
ServiceDesk installer does not set the Email SMTP server Master Setting.	The ServiceDesk installer does not set the settings to support the send email actions. Several features, such as routing rules and report scheduling, require the **Process Manager SMTP Email Master Setting** to be set if emails are to be sent. For the **Send Email** action to work, you must manually set the Master Setting for the SMTP server. **Workaround:** ■ In the Process Manager portal, perform the following actions: ■ Click **Admin > Portal > Master Settings**. ■ On the **Process Manager Settings** page, expand **Email Settings**. ■ In the **SMTP Server** field, type the correct SMTP server address. ■ To test the connection, click **Ping**. ■ On the **Message from webpage** dialog box, click **OK**. ■ When you are finished, scroll to the bottom of the page and click **Save**.	
ServiceDesk installer does not consistently capture the underscores that are used as part of server or service account names.	The ServiceDesk installer does not consistently capture and render the underscores (_) when they are used in the names of servers or service accounts. For example: The server name is typed **<cherry_smp>**. The server name is displayed in the installer as **cherrysmp**.	TECH199410

Table 1-7   Known issues *(continued)*

Issue	Description	Article link
Running a repair on ServiceDesk reverts the **OnIncidentReceived** ruleset to its default state.	Using the ServiceDesk installer to repair ServiceDesk reverts the **OnIncidentReceived** ruleset to its default or out-of-the-box state. The repair reinstalls the single default rule in the **OnIncidentReceived** ruleset. **Workaround:** If you must repair ServiceDesk, take note of all the rules that were added to the **OnIncidentReceived** ruleset. These notes should include the conditions and actions that are used in each of the rules. After you run the repair, add the rules back to the **OnIncidentReceived** ruleset.	
No default report is provided to display the incidents that are on hold.	After an incident is placed on hold, it disappears from reports and task lists. No default report is provided to display the incidents that are on hold.	TECH199688
Adding groups to and removing groups from Service Queues does not affect currently assigned incidents.	The group-to-service queue relationship is only used during ticket assignment. Adding groups to and removing groups from Service Queues only affects future assignments and does not affect currently assigned incidents. **Workaround:** Individual ticket assignments can be reset when you reassign them to the queue to which they are currently assigned.	
Deleting a Service Queue can cause routing rules to fail.	If you delete a service queue before you modify the routing rules that route incidents to that queue, the routing rules error out. **Workaround:** Before you delete a service queue, modify all the rules that route incidents to the queue and route them to another queue.	
Deleting a Service Queue does not affect existing ticket assignments.	If a service queue is deleted, all existing tickets stay assigned to the service queue's groups. **Workaround:** Individual ticket assignments can be reset when you reassign them to a different queue.	
Service Queues do not detect newly created groups.	Opening the **Create/Edit Service Queue** page caches the existing ServiceDesk groups. The Service Queues do not detect newly created groups.	TECH198039

Table 1-7   Known issues *(continued)*

Issue	Description	Article link
Send Email action is displayed twice in the **Add Action** drop-down list for **Process Event** rulesets.	When you create rules for Incident Management Process Event rulesets, the **Send Email** action appears twice in the **Add Actions** drop-down list. You can use both **Send Email** actions. Both actions produce the same results.	
The Change Request form's **Location Search** does not find locations. It can cause an **application error**.	The Change Request form's **Location Search** functionality does not discover locations. The search functionality also populates the **Search the CMDB** field with your location search criteria. When you clear the **Search the CMDB** field and try to search the CMDB for the equipment and services that the change affects, an **application error** is thrown. Your change request is canceled. **Workaround:** ■ Request a change. ■ Type a title, description, and justification. ■ In the **Location** field, type in the location and use the auto-complete functionality of this field to select the location. Do not use the **Search** function to search for a location. ■ As you progress through the creation of your change request, the **Search the CMDB** field is not prepopulated. You can search for the equipment and services that the change affects without receiving an **application error**.	
Change Implementers cannot assign implementation tasks when using the **Manage Implementation Task** action.	Members of the Change Implementer group receive an error when they use **Manage Implementation Task** on the change request ticket's **Process View** page to assign implementation tasks. Task assignment does not grant permissions. Task assignment uses the actual user's permissions. **Workaround:** **Option 1:** ■ Create a Change Implementer's group. ■ Make sure to assign the group the **WorkflowTasksManagement.Add** permission. ■ Add change implementers to the change implementer group. **Option 2:** ■ Grant the change implementer administrative permissions.	TECH199363

Table 1-7   Known issues *(continued)*

Issue	Description	Article link
Change Managers cannot add a new CAB.	Members of the Change Manager group receive an error when they try to add a new CAB. Change Manager group does not have the **AccountManagement.Access** permission. **Workaround:** Grant the **AccountManagement.Access** permission to the Change Manager group.	
Change managers cannot add a category or a bulletin board when adding a bulletin board entry.	Members of the Change Manager group receive an error when they click **Add Category** or **Add Bulletin Board** on the **Add Bulletin Board Entry** page. Change Manager group does not have the **Articles.CanAddCategory** and the **Articles.CanAddArticle** permissions. **Workaround:** Grant the **Articles.CanAddCategory** and the **Articles.CanAddArticle** permissions to the Change Manager group.	
Change request ticket's **Process History** does not display the execution of the automation rules.	When you open a change request ticket's **Process View** page, the execution of the automation rules is not displayed in the **Process History** section. By default, the **Process Messages** filter is turned off. **Workaround:** ■ Open a change request ticket. ■ On the ticket's **Process View** page, in the **Process History** section, click **Filter**. ■ In the **Filter Options** dialog box, in the **Messages** section, check **Process Messages** and then click **Apply**. ■ The **Process History** section on your change tickets' **Process View** page displays the automation rules execution.	
Support users cannot post **Time Spent** working on an incident.	Members of the support group do not have permissions to post **Time Spent** working on the incident in the **Start/Stop Process Timing** section on the **Process View** page. **Workaround:** Open the incident ticket, click **Work Incident**, and use the **Specify Time Worked** feature on the **Incident Response** page.	

	Table 1-7	Known issues *(continued)*

Issue	Description	Article link
False failure can be reported on knowledge base article creation.	When you create a knowledge base article from a problem, a failure is reported even though the article was created successfully. To verify that the article was created successfully, navigate to the **Knowledge Base** page and search for the article.	
Known Issue article can be populated with *"data name Problem.CreateDate is not valid because piece CreateDate does not exist. This typically happens if the data type changes structure"*.	When you resolve a problem by creating a known issue, the Known Issue article is created. However, the **Reported Problem** field in the Known Issue article is populated with *"data name Problem.CreateDate is not valid because piece CreateDate does not exist. This typically happens if the data type changes structure"*. **Workaround:** ■ Navigate to the **Knowledge Base** page and open the Known Issue article. ■ On the **KB Known Issue** page, click the **Actions** symbol (orange lightening) and then click **Edit Entry**. ■ On the **KB Edit Article Entry** page in the **Text** field, edit the information in the **Reported Problem** line and click **Save**.	
Process Manager portal crashes when an end-user searches for articles in the knowledge base.	An end user has default access to the **Knowledge Base** page in the Process Manager portal, but does not have rights to any article categories. When the end user uses the **Knowledge Base** page's **Search Articles** feature, the Process Manager portal crashes. The end user must restart the session. **Workaround:** Option 1: ■ Configure the end user's permissions so that access is removed to the **Knowledge Base** page. Option 2: ■ Configure the end user's permission so that access is granted to at least one knowledge base article category.	
You cannot use the **KB Migration Wizard** to migrate user created Helpdesk Solution 6.5 knowledge base articles .	The **Migrate KB Articles from Helpdesk 6.5** option does not import user-created Helpdesk Solution 6.5 knowledge base articles . The KB Migration Wizard is intended for importing Helpdesk Solution 6.5 knowledge base content that was added through the installation of a KBI solution add-on.	TECH162732
You cannot run the **Migrate KB Articles from Helpdesk 6.5** process.	Using the **Migrate KB Articles from Helpdesk 6.5** option to migrate the Helpdesk Solution 6.5 knowledge base content fails. No knowledge base items are migrated and errors are thrown in the log.	TECH199272

Table 1-7 Known issues *(continued)*

Issue	Description	Article link
You cannot run the **Migrate Helpdesk 6 Incidents** process.	Using the **Migrate Helpdesk 6 Incidents** option throws an error *Invalid Portal Permissions*. The instructions that are displayed in the error message do not resolve the issue.	TECH199274
False failure may be reported on a submitted incident.	The first submitted incident after a new install of ServiceDesk 7.5 or an IISRESET reports an error even though the incident was submitted successfully.	
ServiceDesk may not correctly connect to the inbound mail server when the POP protocol is used.	In some email environments, ServiceDesk does not correctly connect to the inbound mail server using the POP protocol. Error message may display: *"Connection to endpoint failed: An error occurred while communicating with the server [Index and length must refer to a location within the string. Parameter name: length]. Do you need to enable SSL?"* **Workaround:** Use IMAP instead of POP.	
You cannot use the ServiceDesk installer to use SSL (https://) to configure the Process Manager database.	In the ServiceDesk Installer on the **Set Server Base URL** page, the **Use SSL (https://)** check box does not work correctly. It does not configure the Process Manager database using SSL (https://). **Workaround:** After you install ServiceDesk, enable SSL (https://).	TECH199946
Some variables in Incident and Change Management email templates may not work properly.	When you create an Incident or Change email template and add variables to it, some variables may not populate correctly and may contain incorrect information.	TECH200230
The **Task Response Url** variable in Incident Management email templates does not work.	When you add the **Task Response Url** to an Incident Management email template, an invalid link to the incident ticket is created in the email.	
In Problem Management, all **List Open Problems...** reports and all **Problems Closed...** reports do not display ticket data.	The Problem Management **List Open Problems...** reports and **Problems Closed...** reports do not extract the correct data. **Workaround:** Edit the report that you want to use so that it extracts the correct data.	TECH200490

Table 1-7	Known issues *(continued)*	

Issue	Description	Article link
Using the **Hold Management** Smart Task to place an Incident on hold, may result in an unworkable ticket.	If you use the **Hold Management Smart Task** to place a ticket on hold after you use the **Edit Incident Process Action** to edit the ticket, the ticket becomes unworkable and unrecoverable. ■ The ticket's process history displays that the **OnTicketPlacedOnHold** ruleset was run. ■ No **Remove from Hold** task is created. ■ The ticket does not come off hold when the incident resume date and time is reached. ■ No errors are displayed in the logs.	TECH200965
Automation Rule "to send an email **To Task Assignees** on Task Creation" may not work properly.	**Scenario 1:** When a subtask is created, you want to send an email to notify the subtask assignee. ■ You create an email template for the **Data Event**, **TaskCreated**. ■ You create an Automation Ruleset and a rule to send an email **To Task Assignees** on Task Creation. ■ A subtask is created. ■ Rule runs and evaluates properly and claims to have performed the action successfully. ■ Assignee never receives the email. **Scenario 2:** When any other type of task is created, you want to send an email to notify the task assignee. ■ You create an email template for the **Data Event**, **TaskCreated** ■ You create an Automation Ruleset and a rule to send an email **To Task Assignees** on Task Creation. ■ Rule runs and evaluates properly and claims to have performed the action successfully. ■ Assignee may or may not receive the email.	
The Automation Rule's **Any group satisfies** option does not produce expected results.	When you use the **Any group satisfies** option in a rule to include multiple groups, even if all groups are false, the rule still executes the action(s). **Workaround:** Use the **All groups must be met to satisfy** option and create separate rules for each group.	

Table 1-7   Known issues *(continued)*

Issue	Description	Article link
The Automation Rule's **Any condition satisfies** option does not produce expected results.	When you use the **Any condition satisfies** option in a rule to include multiple conditions in the same group, even if all conditions are false, the rule still executes the action(s). **Workaround:** Use the **All conditions must be met to satisfy** option and create separate rules for each condition.	
The Automation Rule's Ruleset Action "to set the priority of an incident using the Impact/Urgency Matrix" fails.	When you create a rule to set the priority of an incident using the Impact/Urgency Matrix, the Action fails even if the condition is met.	

Fixed issues

The following are the previous issues that were fixed in this release.

Table 1-8   Fixed issues

Issue	Description
Installation issues can occur if you do not manually uninstall any previous 7.5 Beta builds. (Beta customers)	Previously, ServiceDesk MSI did not overwrite the `ServiceDeskSetup.exe` on upgrade. Installing ServiceDesk on a server where a previous version was installed did not update the setup files from the previous installation.
When you schedule a change, a link to view the change request does not get created on the **Calendar** page.	Previously, the Change Management process did not populate the URL field. Because the URL field did not get populated, a link to view the change request ticket did not get created on the **Calendar** page
If you create a change request from a problem and the change fails, the problem ticket is unworkable.	Previously, if you created a change request from a problem and the change failed, the problem ticket remained open with an incomplete task. The problem ticket did not receive the message that the change request had closed., which left the problem ticket in an unrecoverable state
Incident Management ticket application error	Previously, after you clicked on a computer that was added to an IM ticket using the advanced form an application error occurred

Table 1-8   Fixed issues *(continued)*

Issue	Description
Report Schedules	Previously, in some circumstances, errors were thrown you attempted to create or run **Report Schedules**.
Change Management Routing Rule	Previously, the **Change Management Routing Rule** condition **Change Plan Type** did not function correctly. Attempting to use this condition in a ruleset, resulted in errors.
OnChangeReceived Change Management Ruleset errors	Previously, using the **Affected Assets** condition in the **OnChangeReceived Change Management Ruleset** produced unexpected results.
Routing rules issue	Previously, Email Templates were stored within the routing rules and did not update when templates were changed. When you created routing rules using the **Send Email** action, email template changes required the rule to be re-saved.
ReOpen Incident box does not allow entry for Reason to re-open in the `SD.ReopenIncident` Project .	Previously, you were unable to enter the **Reason for ReOpening**, which removed the ability to click the **Reopen** button.
Migrate Helpdesk Incidents not working correctly.	Previously, the **Migrate Helpdesk Incidents** process did not function correctly. When you ran the process, it did not indicate any errors but no tickets were migrated.
POP Blacklist issue	Previously, Email Monitoring: Using the Blacklist option while running POP email monitoring caused the server to stop processing additional emails. Symantec recommended using IMAP for email monitoring if you wanted to use the Blacklist function.
Non-ASCII characters in computer names.	Previously, at the end of the ServiceDesk installation, you clicked **Open ServiceDesk**. An error was displayed if the computer name contained non-ASCII characters.

Other things to know

The following are things to know about this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-9   Things to know

Component	Issue	Article link
Symantec™ ServiceDesk Solution 7.5 may not appear in the **Available Products** list in the Symantec Installation Manager (SIM).	The **Symantec™ ServiceDesk Solution 7.5** may not appear in the **Available Products** list because the Symantec Installation Manager (SIM) is pointed to a previous release's or a Beta release's product listing (PL). **To point SIM to the current PL:** 1 Open SIM. 2 On the **Install New Products** page, click **Cancel** to change the product listing (PL). 3 In the **Symantec Installation Manager** dialog box, click **Yes**. 4 On the **Install Products** page, click **Settings**. 5 On the **Settings** page, click **Change product listing**. 6 On the **Manage Product Listings** page, check **itms_7_1_SP2** and click **Edit**. 7 In the **Edit Product Listing** dialog box in the **Path** field, update the product listing (PL) to point to: http://www.solutionsam.com/solutions/pl/symantec_v2.pl.xml.zip.	
You cannot use a non-default HTTP port to install Workflow.	Using a non-default HTTP port to install Workflow causes an error for prerequisite failure to occur and the ServiceDesk installation to fail.	
Incident Management	Incident Management requires setup and is not fully functional out-of-the-box. See the *About configuring ServiceDesk* topic.	See the Symantec™ ServiceDesk 7.5 Implementation Guide or the Symantec™ ServiceDesk 7.5 User Guide.
Change Management	Change Management requires setup and is not fully functional out-of-the-box. See the *About configuring ServiceDesk* topic.	See the Symantec™ ServiceDesk 7.5 Implementation Guide or the Symantec™ ServiceDesk 7.5 User Guide.
You cannot adjust the incident verification timeout period.	The Incident Management incident verification timeout period is three days.	

Table 1-9   Things to know *(continued)*

Component	Issue	Article link
Send Email link on the Incident Management **Process View** page	The **Send Email** link on the Incident Management's **Process View** pages is hidden until an email template is created. See the *Creating email templates for Incident Management* topic.	See the Symantec™ ServiceDesk 7.5 User Guide.
Send Email link on the Change Management **Process View** page	The **Send Email** link on the Change Management's **Process View** page is hidden until an email template is created. See the *Creating email templates for Change Management* topic.	See the Symantec™ ServiceDesk 7.5 User Guide.
Improved security controls on the Workflow Server	Symantec has improved security controls on the Workflow Server. The improved security can potentially block the ability to deploy from a local Workflow Designer to a remote Workflow Server. If you cannot deploy to a remote Workflow Server, change the following setting on the remote Workflow Server before attempting to deploy. **To allow remote connections:** ■ On the Workflow Server, right-click on the **Task Tray Tool** and click **Settings**. ■ In the **Workflow Server** section next to **Workflow Server Configuration**, click the ellipsis. ■ In the **General** section, check **Allow Remote Connections**. Please note that the Symantec security best practice is to revert this setting after you are finished deploying. For more information on Symantec security best practices, see the article *ServiceDesk/Workflow General Security Best Practices*.	www.symantec.com/docs/DOC6160
IT Analytics 7.1 SP2	ServiceDesk 7.5 is not compatible with IT Analytics 7.1 SP2. If you want to use IT Analytics 7.1 SP2 with ServiceDesk 7.5, a ServiceDesk Pack 7.5 for IT Analytics 7.1 SP2 is available. For more information, see the *ServiceDesk Pack for Altiris™ IT Analytics 7.1 SP2 from Symantec™ User Guide (ServiceDesk 7.5)*.	www.symantec.com/docs/DOC5639

Table 1-9 Things to know *(continued)*

Component	Issue	Article link
ServiceDesk Solution Software User Guide	The *ServiceDesk Solution Software User Guide* has been deprecated for this release. The instructions that were in this guide are now in the *ServiceDesk Implementation Guide* and *ServiceDesk User Guide*.	See the Symantec™ ServiceDesk 7.5 Implementation Guide or the Symantec™ ServiceDesk 7.5 User Guide.
ServiceDesk Portal User Guide	The *ServiceDesk Portal User Guide* has been deprecated for this release. The instructions that were in this guide are now in the *ServiceDesk User Guide*.	See the Symantec™ ServiceDesk 7.5 User Guide.
ServiceDesk Customization Guide	The *ServiceDesk Customization Guide* has been deprecated for this release. Because of the changes to ServiceDesk for this release, most of the customizations can be accomplished in the Process Manager portal. Some advance customizations can still be accomplished by editing the workflow processes. See the *Configuring ServiceDesk* and *Advanced ServiceDesk customizations* topics.	See the Symantec™ ServiceDesk 7.5 Implementation Guide or the Symantec™ ServiceDesk 7.5 User Guide.
Cloud-enabled Management	ServiceDesk 7.5 does not support Cloud-enabled Management.	N/A

Documentation that is installed

Table 1-10　　Documentation that is included into the product installation

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■　The F1 key when the page is active. ■　The **Context** command, which is available in the Symantec Management Console on the **Help** menu.
User Guide	Information about how to use this product. This information is available in PDF format.	■　The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■　The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Other information

Table 1-11　　Information resources that you can use to get more information

Document	Description	Location
Symantec Management Platform 7.1 SP2 User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page

Table 1-11   Information resources that you can use to get more information
(continued)

Document	Description	Location
Symantec Management Platform 7.1 SP2 Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform 7.1 SP2 Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	Symantec Management Platform 7.1 SP2 Installation Guide
Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Administration Guide	Information about using the Symantec Management Platform.	Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Administration Guide
Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Release Notes
Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Installation and Upgrade Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	Symantec™ IT Management Suite 7.5 powered by Altiris™ technology Installation and Upgrade Guide
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page